PUBLIC KEY VALIDATION SERVICE

Abstract of the Disclosure

A public key validation agent (PKVA) includes a registration authority

5   which issues a first unsigned public key validation certificate (unsigned PKVC)

off-line to a subject that binds a public key of the subject to a first public key

serial number (PKVN).   The registration authority maintains a certificate

database of unsigned PKVCs in which it stores the first unsigned PKVC. A

credentials server issues a disposable public key validation certificate

10   (disposable PKVC) on-line to the subject. The disposable PKVC binds the

public key of the subject from the first unsigned PKVC to the first PKVN from

the first unsigned PKVC. The credentials server maintains a table that contains

entries corresponding to valid unsigned PKVCs stored in the certificate database.

The PKVA can be employed in a public key validation service to validate the

15   public key of the subject before a private/public key pair of the subject is used

for authentication purposes.

"Express Mail" mailing label number: EL546309171us

Date of Deposit: Jan. 13, 2001

I hereby certify that this paper of fee is being deposited with the
United States Postal Service "Express Mail Post Office to Addresses"
service under 37 CFR 1.10 on the date indicated above and is
addressed to the Assistant Commissioner for Patents,
Washington, D.C. 20231.

Printed Name Patrick G. Billig

Signature